Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 24 July 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

[For info click here](http://www.whitehouse.gov/homeland)
www.whitehouse.gov/homeland

Daily Overview

- Microsoft has released "Security Bulletin MS03−030: Unchecked Buffer in DirectX Could Enable System Compromise (Critical)," and a patch is available on the Microsoft Website. (See item 21)

- Microsoft has released "Security Bulletin MS03−031: Cumulative Patch for Microsoft SQL Server (Important)," and a patch is available on the Microsoft Website. (See item 22)

- CNET News.com reports that Swiss researchers released a paper Tuesday outlining a way to speed the cracking of alphanumeric Microsoft Windows passwords, reducing the time to break such codes to an average of 13.6 seconds from 1 minute 41 second. (See item 23)

- The Associated Press reports that a gunman opened fire during a meeting inside New York's City Council chambers Wednesday killing Councilman James Davis. (See item 24)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base

Service Industries: Banking and Finance; Transportation; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information and Telecommunications; Internet Alert Dashboard

Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *July 23, Associated Press* — **Violent storm kills three, cuts power. Ohio and Tennessee valleys suffered much damage from a strong storm front caring winds blowing at speeds between 60 and 100 mph. At least three people were killed, up to 300,000 people are without electricity,** and homes and businesses were badly damaged. **Memphis International Airport (MIA) was essentially shut down due to power outages, and flights diverted to other cities.** Northwest Airlines, which has a hub at MIA, has advised customers with

connecting flights through Memphis to delay their travel plans through Sunday, July 26. Northwest expects regular flights to be back to normal by Wednesday evening. In Memphis, Tennessee, a 500−foot crane being used to build a new sports arena was left leaning by the strong winds. Authorities closed the Beale Street entertainment district for fear that the crane might topple.
Source: http://abcnews.go.com/wire/US/ap20030723_319.html

2. *July 22, Energy Info Source* — **AEP completes restoration of service for major areas hit by hurricane Claudette. American Electric Power has restored power to most customers in their service area along the gulf coast of Texas affected by hurricane Claudette. All major transmission and distribution infrastructure is operational, except for isolated pockets of power outages affecting about 100 customers,** almost half of whom are in the city of Victoria, TX, located approximately 100 miles southwest of Houston. Approximately 72,000 electricity consumers lost power during the hurricane. The storm knocked down or damaged 23 transmission lines and more than 300 distribution poles.
Source: http://www.energyinfosource.com/aoi/news−details.cfm?id=1952 0&FLink=

[Return to top]

Chemical Sector

3. *July 17, The Pennington Post (NJ)* — **Chemical labor issues discussed with Bush Administration in Trenton. The New Jersey Department of Labor has projected that labor for the chemical industry will fall 7.5 percent in the period ending 2010, a development that influences concerns in New Jersey as well as the national market.** "Chemical manufacturing holds 74,000 jobs in this state alone, it is the number one export in this state and the number one export of the nation," Linda Conlin, assistant secretary of Commerce for Trade Development said. **In reaction to these startling projected figures, the Bush administration hosted a manufacturing roundtable in Trenton on July 8, 2003 to discuss issues involving the local chemical manufacturing industry.** Conlin led the discussion about the government's role in this declining industry, which involved nine panelists that all had a stake in New Jersey chemical manufacturing. Nearly 30 roundtables such as this one are being held by the Bush administration, in hopes of collecting information from those that work directly in the industry.
Source: http://www.zwire.com/site/news.cfm?newsid=9862244&BRD=1689&PAG=461&dept_id=41795&rfi=6

[Return to top]

Defense Industrial Base Sector

4. *July 23, The Philadelphia Inquirer* — **Army plans new Guard call−up to relieve weary troops in Iraq. The U.S. Army has developed a plan to relieve troops in Iraq by bringing in U.S.−based units and by calling up 10,000 National Guardsmen to active duty.** The plan calls for units in Iraq, Afganistan, and other countries where the U.S. has peacekeeping forces, to be rotated home after one year. The plan will require the call−up of two specially trained

"enhanced brigades" of the Army National Guard to be included in the rotation for a one−year tour in Iraq. Of its 33 active−duty brigades, 21 are deployed overseas: 16 in Iraq, two in Afghanistan, two in South Korea and one in Bosnia. **Military officials are hoping that the foreign coalition forces will increase from 19,000 to 40,000 troops by the end of the year.** Source: http://www.philly.com/mld/inquirer/news/nation/6361461.htm

[Return to top]

Banking and Finance Sector

5. *July 23, The Telegraph (UK)* — **Austria accuses North Korean bank of spying. North Korea's only bank in Europe, the Golden Star Bank in Vienna, Austria, is being used as a base for North Korean secret services, according to a report by the Austrian authorities.** According to the report, "there are detectable efforts by the North Korean secret services to place its agents in diplomatic and non−diplomatic positions in Austria. The camouflage for these activities is Europe's only established branch of the North Korean state bank, which is located in Vienna, as well as martial arts clubs established around the country." **The Austrian government will not close the bank, even though it is also suspected of being involved in money laundering and attempts to finance Pyongyang's military program, because the government had not yet secured enough evidence to shut the operation down.** The Golden Star Bank is linked to the regime in Pyongyang's illegal selling of minerals and ginseng, in which North Korea has a virtual monopoly. The report that the Golden Star Bank was under scrutiny was confirmed by Rudolf Gollia, a spokesman for the Austrian interior ministry. Source: http://money.telegraph.co.uk/money/main.jhtml?xml=/money/2003/07/23/cnkor23.xml&menuId=242&sSheet=/money/2003/07/23/ixfr ontcity.html

[Return to top]

Transportation Sector

6. *July 23, Washington Post* — **Last−minute booking gets more popular.** For more than 20 years after deregulation, the airlines used their superior technology to gain pricing power over their customers. Now, thanks to the Internet, the very tool that the airlines use most, travelers have that power. **Frequent business travelers have taken what they've learned about finding cheaper tickets online or waiting for last−minute fare sales into planning personal trips.** These smart travelers are reducing the airlines' ability to raise business fares and wrecking their long−held pricing models. **Gerard J. Arpey, American Airlines president and chief executive, told airline analysts last week that travelers are booking "much more close−in than they have historically." That means American is now having trouble distinguishing business travelers from leisure travelers.** Airline officials say that when vacationers book months in advance the carrier knows how many seats it should leave open for last−minute passengers −− who it normally assumes would be business travelers willing to pay higher fares −− and how many to put on sale. **Travel expert Terry Trippler of Cheapseats.com said the airlines' recent financial troubles have made some travelers leery of booking too far in advance. That's because airlines continue to cut flights, so a flight and even a destination booked months in advance may no longer be flown.**

Source: [http://www.washingtonpost.com/wp−dyn/articles/A26036−2003Jul 21.html?nav=hptoc_c](http://www.washingtonpost.com/wp−dyn/articles/A26036−2003Jul21.html?nav=hptoc_c)

7. *July 23, Knoxville News−Sentinel* — **Second “black box” for aircraft. To allow quicker findings of the causes of commercial airline crashes, U.S. Rep. John J. Duncan, Jr. said that he wants Congress to force future aircraft to have a second, improved "black box" full of recorded information.** Duncan, a Knoxville Republican and former chairman of the House aviation subcommittee, on Tuesday filed a bill, H.R. 2632, that aims to avoid past problems of not finding the box with recordings of sounds (including any explosions), cockpit staff conversation and flight control data or having to spend two weeks or more and millions of dollars to locate it. **"If we have another commercial aviation disaster, we will need to know immediately if it is a terrorist attack," Duncan said.** The second so−called "black box" − both actually would be orange − would be an improved model over the current one at the front of commercial aircraft, both Duncan and Jim Hall, former chairman of the National Transportation Safety Board, said. **It would record the last two hours of a flight's activity − rather than the current 30 minutes − have an emergency power supply (none for the current model) and be mounted on the tail and automatically ejected away from a crashing plane and float on water, they said.**
Source: http://www.knoxnews.com/kns/national/article/0,1406,KNS_350_2129930,00.html

8. *July 22, Federal Computer Week* — **New rules for ground cargo.** Security officials want to know what's being shipped on the ground before it gets here. **The Homeland Security Department proposed new rules Tuesday that would require all truck and rail cargo to provide advance electronic information on their shipments. Security officials had required only air and sea shipments to provide advance information before arriving in the United States.** Deadlines for providing the information would depend on the cargo's transportation method, and if it's imported or exported. Railroads, for example, would have to submit manifests two hours before arriving at a U.S. port, and truckers would have to submit content lists two hours before arriving at a border to leave the United States. **The land cargo manifests would be part of an electronic repository already in development for air and sea shipments. The database is expected to be operational later this year.** There is a 30−day waiting period for public comment on the new rules before the agency can formally adopt them.
Source: http://www.fcw.com/fcw/articles/2003/0721/web−cargo−07−22−03 .asp

[Return to top]

Postal and Shipping Sector

9. *July 22, Puget Sound Business Journal* — **Waiting period over in Airborne's proposed DHL merger. Airborne Inc., the parent company of package shipper Airborne Express, said its merger with DHL Worldwide Express Inc. can proceed now that the waiting period under the Hart−Scott−Rodino (HSR) Antitrust Improvement Act has expired.** "At this time, the HSR Act no longer prohibits the parties from closing the proposed transaction," the companies said in a statement. **Airborne shareholders are scheduled to vote on the $1.05 billion merger August 14.** The company didn't say whether the waiting period affects an ongoing review by a U.S. Department of Transportation administrative law judge questioning whether the company is violating laws limiting foreign ownership of domestic airlines. **Though the**

deal does not include Airborne's air shipment subsidiary, ABX Air Inc., that business would derive nearly all of its post−merger revenue from agreements made with Deutsche Post, effectively giving Germany's Deutsche Post control.
Source: http://seattle.bizjournals.com/seattle/stories/2003/07/21/da ily16.html

[Return to top]

Agriculture Sector

10. *July 23, Reuters* — **EU backs farmers who want to grow GM crops. Local or national governments cannot ban farmers from planting genetically modified crops, the European Commission said on Wednesday, supporting those farmers who want to embrace the technology.** The Commission's new guidelines, part of a push to end the five−year moratorium on GMO crops, spell out how crops produced from genetically modified organisms can be grown alongside organic and conventional crops within the European Union. "It is not possible for regions or national governments to introduce GMO−free zones," European Farm Commissioner Franz Fischler said. **However, Fischler said there could be an opt−out in cases where it was impossible to limit contamination of non−GM crops due to the variety of biotech crop being sown and the lay−out of fields.**
Source: http://www.alertnet.org/thenews/newsdesk/L23215637.htm

11. *July 23, Illinois Ag Connection* — **Researchers move ahead on ways to control rust. Asian soybean rust has long been a factor limiting soybean production in Australia and parts of Asia. Yield losses of more than 80 percent have been reported from experimental trials in that region, with losses of 30 to 50 percent commonly reported from producers' fields.** "In recent years, the disease has spread to Hawaii, Africa, and South America," said Monte Miles, plant pathologist with the Agricultural Research Service. **While not yet found in the U.S., the recent introduction of the disease into South America raises the danger that it could be spread here in the near future. "A computer simulation risk assessment showed that Asian soybean rust could cause yield losses of 10 to 50 percent in U.S. production if the disease became established**. It is critical that our soybean industry be prepared to combat this disease before it arrives here," said Miles. With support from the U.S. Department of Agriculture (USDA) and the United Soybean Board, Miles is collaborating with scientists from Iowa State University, USDA's Foreign Disease−Weed Science Research Unit, and researchers in six countries where the disease occurs, in a concerted effort aimed at testing the options for controlling this disease and developing new sources of genetic resistance.
Source: http://www.illinoisagconnection.com/story−state.cfm?Id=561&y r=2003

[Return to top]

Food Sector

12. *July 23, CBS News* — **FDA plans more inspections.** To ensure the nation's food supply is safe from terrorists, the U.S. Food and Drug Administration (FDA) has announced it will increase inspections of imported food this year. **U.S. Secretary of Health and Human Services Tommy Thompson says the FDA will conduct five times the number of imported food**

inspections this year than it did two years ago, rising steadily from 12,000 in 1991 to 62,000 this year. Also, he says, the FDA will inspect more than twice the number of ports of entry this year, from 40 to 90 inspections. To see that the quotes are met, the FDA hired more than 650 additional people for food security and safety, according to Thompson.
Source: http://www.cbsnews.com/stories/2003/07/22/earlyshow/health/m ain564573.shtml

13. *July 23, Wisconsin Ag Connection* — **EU approves tougher GM labeling rules.** European Union (EU) agriculture ministers have adopted tougher labeling rules on new genetically modified (GM) foods. **The new rules could mean new biotech products could be sold in Europe this fall. U.S. officials said the new rules would do little to remove barriers on new genetically altered products in the European market.** Under the new rules, all genetically altered products including animal feed, vegetable oils, seeds and byproducts containing more than 0.9% genetically altered material will have to be clearly labeled with the words, "This product is produced from Genetically Modified Organisms." A new register will be created that will mandate that businesses dealing in GM products trace each GM product from its point of origin to the supermarket shelf. The EU's new European Food Safety Authority will assess the safety of all new biotech products before they are allowed to be sold.
Source: http://www.wisconsinagconnection.com/story−national.cfm?Id=7 93&yr=2003

[Return to top]

Water Sector

14. *July 22, Rocky Mountain News* — **Denver Water Board considers drilling wells as insurance. Denver Water, in Colorado, could tap aquifers for emergency water supplies, but such a program would cost the utility $65 million, according to a preliminary report.** "This system would act as an insurance policy in case of some catastrophic failure of our system," said David Little, a Denver Water planner. **If the board approves the underground water plan, it could take 10 to 30 years to develop, Little said. The underground system would require the drilling of 127 wells in various city parks**. Early estimates indicate the wells could generate about 29,000 acre−feet of water annually, enough to serve as many as 60,000 families for a year. **Such a supply represents only a fraction of the 285,000 acre−feet Denver's 1.2 million customers use each year.** Underground water supplies in the Denver Basin are coming under increasing scrutiny because of the lingering drought. But estimates of how much water actually lies beneath Denver and other Front Range cities vary widely. **Denver Water officials believe aquifer water supplies are sharply limited and would require extensive, high−priced treatment in order to drink**. And unlike Denver's standard supplies **underground supplies are considered finite and difficult, if not impossible, to replenish.**
Source: http://rockymountainnews.com/drmn/local/article/0,1299,DRMN_ 15_2126438,00.html

[Return to top]

Public Health Sector

15.

July 22, NBC4 Washington — **Government prepares for bioterrorism threat. The U.S. Centers for Disease Control and Prevention (CDC) has identified many biological threats, highlighting the six of highest priority. Anthrax is an acute infectious disease caused by the bacterium Bacillus anthracis.** The disease is not communicable, but it can be spread in three ways by cutaneous infection, inhalation, and ingestion. **Botulism** is a muscle−paralyzing disease caused by a toxin made by a bacterium called Clostridium botulinum. The toxin poses the largest threat when in food. **Pneumonic plague,** which is caused by the bacterium Yersinia pestis is contagious, and an aerosol attack of the pneumonic plague could reach a large number of people. **Smallpox** generally requires direct face−to−face contact to spread from one person to another. Smallpox can also be spread through direct contact with infected bodily fluids or contaminated objects. **Tularemia** is an infectious disease caused by a hardy bacterium, Francisella tularensis, found in animals, especially rodents and rabbits. In general, the term **"viral hemorrhagic fever"** is used to describe a severe multisystem syndrome. Many of these viruses cause severe, life−threatening disease. **The CDC has outlined second−priority and third−priority bioterrorism threats as well.**
Source: http://www.nbc4.com/news/1879607/detail.html

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

16. *July 23, The Union City Reporter (NY)* — **'Citizen's fleet' soon to be a reality. Since 9/11, more and more citizens have been willing to personally participate in preparing for emergencies in the tri−state area.** Dr. Michael Weinstein, president of the New Jersey Marine Sciences Consortium (NJMSC), with the aid and the full support of the of the U.S. Coast Guard, is developing a citizens' fleet comprised of volunteers whose private vessels could transport people and supplies from or to lower Manhattan in case of an attack or another extreme sudden emergency. **The fleet will go under the name Harbor Emergency Response Organization (HERO). According to Weinstein, the fleet will operate under the guidance of the captain of the port and the Coast Guard and will be mobilized to serve as a supplemental resource to the first responders and other emergency preparedness personnel. The Coast Guard is the lead governmental agency when it comes to marine homeland security.** According to Weinstein, in the immediate aftermath of 9/11, nearly 800,000 people were evacuated from lower Manhattan. Yet, it became abundantly clear just how vulnerable the island was to large−scale attack, and the inherent difficulties in managing the movement of people, emergency supplies and equipment to and from Ground Zero. These difficulties might be infinitely compounded with more generalized attacks at multiple locations.
Source: http://www.zwire.com/site/news.cfm?newsid=9616867&BRD=1295&PAG=461&dept_id=142205&rfi=6

17. *July 23, SignOnSanDiego.com* — **Terror−response drills start at Miramar.** Military

personnel and civilian public safety workers will take part today in a series of drills at Marine Corps Air Station Miramar, CA, to test their readiness to respond to acts of terrorism. Residents near the air station were warned not to be alarmed by noises related to the drills. **The series of four−hour drills will include procedures for dealing with an attack involving weapons of mass destruction, Miramar officials said. Taking part in the drill, dubbed the Naval Integrated Vulnerability Assessment, are Miramar first responders, San Diego County emergency medical service coordinators, and the San Diego HAZMAT team.** The exercise is intended to validate emergency response procedures, determine resource shortfalls and identify areas for improvement, Miramar officials said.
Source: http://www.signonsandiego.com/news/metro/20030723−0636−miram ar.html

18. *July 21, Federal Computer Week* — **Washington, DC readies new telecom network.** Washington, DC, will activate a citywide emergency response network next month as a result of the federal government's concerns about the city's ability to handle emergencies quickly. **The fiber−optic communications network, called DC−NET, is modeled after similar systems in Portland, OR, and Chicago, but the Washington, DC, system is the first built primarily to protect against terrorist threats.** The city's efforts to build a free−standing network separate from the public switched network was in the works two years before the September 11, 2001, terrorist attacks, but the attacks highlighted the importance of improved emergency communications when Washington, DC's telecommunications system collapsed amid an overload of telephone calls. **The new system will allow emergency responders to receive 911 calls faster and will eliminate areas where firefighters' communication systems currently fail, mostly in older buildings with heavy construction and tunnels.** Overall, the DC−NET fiber optics will connect to more than 300 buildings in the city, including government offices, data centers, police and fire departments, hospitals, and schools. **Officials will activate DC−NET in August. The goal is to have three−quarters of the buildings on the network by the end of the year.**
Source: http://fcw.com/fcw/articles/2003/0721/tec−dc−07−21−03.asp

[Return to top]

Information and Telecommunications Sector

19. *July 23, Federal Computer Week* — **Cybersecurity laws spread. Since fall 2001, at least 24 states have introduced bills and 10 states have passed laws addressing information security**, according to a report released Tuesday, July 22, by the National Conference of State Legislatures (NCSL). For example, **Florida allows police to investigate attacks on protected computers** owned by financial institutions and government agencies. Until January 1, 2006, **California's legislature can hold closed sessions on potential threats of terrorist activity against state−owned personnel and property**, including electronic data. **Michigan imposed penalties against people who use the Internet or telecommunications systems or devices to disrupt critical infrastructure** or government operations.
Source: http://www.fcw.com/geb/articles/2003/0721/web−ncs−07−23−03.a sp

20. *July 23, Microsoft* — **Microsoft Security Bulletin MS03−029: Flaw in Windows Function Could Allow Denial of Service. A flaw exists in a Windows NT 4.0 Server file management function that can cause a denial of service vulnerability**. The flaw results because the

affected function can cause memory that it does not own to be freed when a specially crafted request is passed to it. If the application making the request to the function does not carry out any user input validation and allows the specially crafted request to be passed to the function, the function may free memory that it does not own. As a result, the application passing the request could fail. **By default, the affected function is not accessible remotely, however applications installed on the operating system that are available remotely may make use of the affected function. Microsoft has assigned a risk rating of "Moderate" to this issue** and recommends that system administrators consider applying the security patch
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−029.asp

21. *July 23, Microsoft* — **Microsoft Security Bulletin MS03−030: Unchecked Buffer in DirectX Could Enable System Compromise. There are two buffer overruns with identical effects in the function used by DirectShow to check parameters in a Musical Instrument Digital Interface (MIDI) file**. A security vulnerability results because it could be possible for a malicious user to attempt to exploit these flaws and execute code in the security context of the logged−on user. **An attacker could seek to exploit this vulnerability by creating a specially crafted MIDI file**. If the file was hosted on a Web site or network share the user would need to open the specially crafted file. If the file was embedded in a page the vulnerability could be exploited when a user visited the Web page. If the file was sent using an HTML−based e−mail, the vulnerability could be exploited when a user opened or previewed it. **Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately**.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−030.asp

22. *July 23, Microsoft* — **Microsoft Security Bulletin MS03−031: Cumulative Patch for Microsoft SQL Server.** This cumulative patch includes the functionality of all previously released patches for SQL Server 7.0, SQL Server 2000, MSDE 1.0, and MSDE 2000. In addition, it eliminates three vulnerabilitie. Upon system startup, SQL Server creates and listens on a specific named pipe for incoming connections to the server. **A flaw exists in the checking method for the named pipe that could allow an attacker local to the system running SQL Server to hijack the named pipe** during another client's authenticated logon password. In the same scenario **it is possible for an unauthenticated user who is local to the intranet to send a very large packet to a specific named pipe on which the system running SQL Server is listening and cause it to become unresponsive. A flaw exists in a specific Windows function that may allow an authenticated user the ability create a specially crafted packet that, when sent to the listening local procedure call (LPC) port of the system, could cause a buffer overrun**. If successfully exploited, this could allow a user with limited permissions on the system to elevate their permissions to the level of the SQL Server service account, or cause arbitrary code to run. **Microsoft has assigned a risk rating of "Important" to this issue** and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−031.asp

23. *July 22, CNET News.com* — **Cracking Windows passwords in seconds. Swiss researchers from the Cryptography and Security Laboratory of the Swiss Federal Institute of**

Technology in Lausanne (EPFL) released a paper on Tuesday, July 22, outlining a way to speed the cracking of alphanumeric Microsoft Windows passwords, reducing the time to break such codes to an average of 13.6 seconds from 1 minute 41 seconds. The method involves using large lookup tables to match encoded passwords to the original text entered by a user, thus speeding the calculations required to break the codes. Called a time−memory trade−off, the situation means that an attacker with an abundance of computer memory can reduce the time it takes to break a secret code. **Users can protect themselves against the attack by adding non−alphanumeric characters to a password**. Philippe Oechslin, one of the researchers, said he hadn't notified Microsoft of the issue before publishing the paper.
Source: http://news.com.com/2100−1009_3−5053063.html

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_KLEZ.H** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios−ns), 445 (microsoft−ds), 80 (www), 1434 (ms−sql−m), 4662 (eDonkey2000), 54846 (−−−), 113 (ident), 139 (netbios−ssn), 12072 (−−−), 56403 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

24. *July 23, Associated Press* — **Councilman killed at New York City Hall.** A political rival opened fire during a meeting inside New York's City Council chambers Wednesday, July 23, killing Councilman James Davis of Brooklyn, Mayor Michael Bloomberg announced at an afternoon press conference. **The gunman, identified as Othniel Askew, 31, was then shot and killed by police**. Davis was a retired New York police officer who campaigned to stop violence in black neighborhoods. New York police say that **Davis and Askew entered City Hall through a security checkpoint, but did not pass through metal detectors there because employees, reporters with current press passes and police officers were not required to do so**.
Source: http://www.washingtonpost.com/wp−dyn/articles/A35143−2003Jul23.html?nav=hptop_tb

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.